Reasoning in Description Logic Ontologies for Privacy Management

Adrian Nuradiansyah

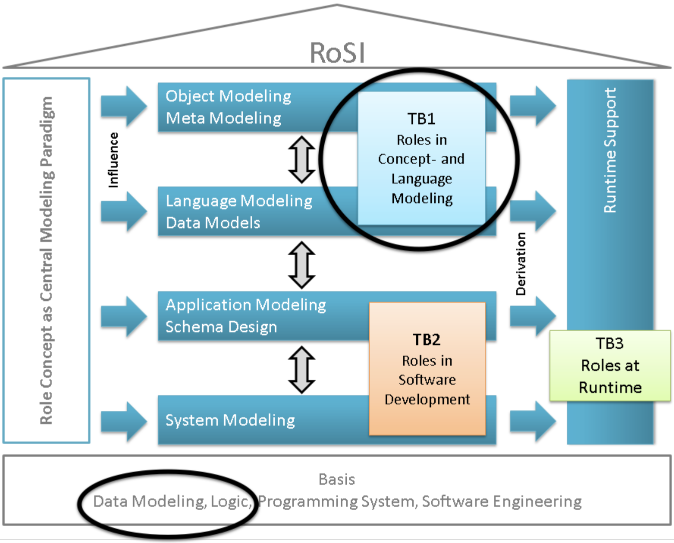
Chair for Automata Theory,
Technische Universität Dresden

13 January 2020

What I am/was

1. Research Assistant at the **Chair for Automata Theory**, Technische Universität Dresden
2. Finished my **Ph.D. study** at TU Dresden, funded by DFG within the **GRK "RoSI"** from 2016 to 2019
3. Completed my **Master study** at TU Dresden in the subject of **Computational Logic** from 2014 to 2016
4. Obtained my **Bachelor degree** at **Universitas Indonesia** in the subject of Information System ("Wirtschaftsinformatik") from 2010 to 2014

Where I was in RoSI



Where I was in RoSI

What our RoSI fellows already did:

- **[Kühn et. al., 2014]** surveyed on a metamodel family for role-based modeling languages
- **[Kühn et. al., 2015]** introduced a context-dependent domain model called "Compartment Role Object Models (CROM)"
- **[Böhme and Lippmann, 2015]** introduced Description Logics of Context (ConDLs) which support, for instance, CROM to perform reasoning
- **[Tirtarasa and Zarriess, 2019]** extended ConDL ontologies with action formalisms

Where I was in RoSI

What our RoSI fellows already did:

- **[Kühn et. al., 2014]** surveyed on a metamodel family for role-based modeling languages
- **[Kühn et. al., 2015]** introduced a context-dependent domain model called "Compartment Role Object Models (CROM)"
- **[Böhme and Lippmann, 2015]** introduced Description Logics of Context (ConDLs) which support, for instance, CROM to perform reasoning
- **[Tirtarasa and Zarriess, 2019]** extended ConDL ontologies with action formalisms

How about **privacy**?

- How do ConDL ontologies deal with privacy policies?
- Considering the complexity of context-based modeling languages, can we start first with the non-context-based settings?

Where I was in RoSI

What our RoSI fellows already did:

- **[Kühn et. al., 2014]** surveyed on a metamodel family for role-based modeling languages
- **[Kühn et. al., 2015]** introduced a context-dependent domain model called "Compartment Role Object Models (CROM)"
- **[Böhme and Lippmann, 2015]** introduced Description Logics of Context (ConDLs) which support, for instance, CROM to perform reasoning
- **[Tirtarasa and Zarriess, 2019]** extended ConDL ontologies with action formalisms

How about **privacy**?

- How do ConDL ontologies deal with privacy policies?
- Considering the complexity of context-based modeling languages, can we start first with the non-context-based settings?

Let's dissect the title of my talk word by word

Reasoning in Description Logic Ontologies
for Privacy Management

Ontologies

- Sharing **common understanding of the structure of information** in various application domains, e.g., Semantic Web or medicine
- **Real examples** of ontologies, such as **SNOMED**, **GeneOntology**, etc
- Provide **semantics** to describe the meaning of the data

Database	**Ontology**
Closed world assumption	Open world assumption
Unique name assumption (UNA) for objects/individuals	No UNA
Schema behaves as constraints on structure of data	Ontology axioms behave like implications (inference rules)

- Ontology's languages are **more expressive** than DB schema languages.
- **Web Ontology Language** (OWL) is the prominent one
- The logical underpinning of OWL $\Rightarrow$ **Description Logics**

Reasoning in Description Logic Ontologies
for Privacy Management

Description Logics

- A family of first-order logic
- Formalism for declarative description of facts/rules
- Powerful reasoning services
  Making something implicit to be explicit facts
- A main concern in DL researches:

Developing/Investigating **(in)expressive** DLs that have **decidable inference problems** that can be solved by **(practical) reasoning procedures**

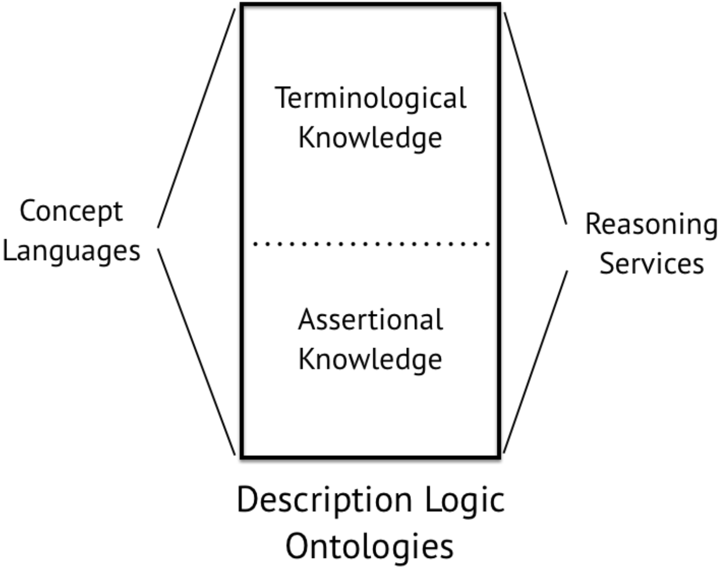
- Representing the conceptual knowledge of an application domain in a well-understood way.

Non-German people who work at an IT Department whose all locations are either in Germany or in Austria

$$\Downarrow$$

$$\neg German \sqcap \exists worksAt.(ITDept \sqcap \forall located.(Germany \sqcup Austria))$$

The Famous Illustration on "Description Logic Systems"



DL Concepts

Name	Syntax	Example
Top	$\top$	*tautology*
Concept Name	A	*Germany*
Conjunction	$C \sqcap D$	$German \sqcap Female$
Disjunction	$C \sqcup D$	$Germany \sqcup Austria$
Existential Restriction	$\exists r.C$	$German \sqcap \exists worksAt.ITDept$
Universal Restriction	$\forall r.C$	$ITDept \sqcap \forall located.Germany$
Negation	$\neg C$	$\neg German$
(One of) Nominal	$\{a_1, \ldots, a_n\}$	$\{LINDA, JOHN, JIM\}$

DL Concepts

Name	Syntax	Example
Top	$\top$	*tautology*
Concept Name	A	$Germany$
Conjunction	$C \sqcap D$	$German \sqcap Female$
Disjunction	$C \sqcup D$	$Germany \sqcup Austria$
Existential Restriction	$\exists r.C$	$German \sqcap \exists worksAt.ITDept$
Universal Restriction	$\forall r.C$	$ITDept \sqcap \forall located.Germany$
Negation	$\neg C$	$\neg German$
(One of) Nominal	$\{a_1, \ldots, a_n\}$	$\{LINDA, JOHN, JIM\}$

$\mathcal{ALC}$

- Closed under Boolean operators
- Intractable

DL Concepts

Name	Syntax	Example
Top	$\top$	*tautology*
Concept Name	A	*Germany*
Conjunction	$C \sqcap D$	$German \sqcap Female$
Disjunction	$C \sqcup D$	$Germany \sqcup Austria$
Existential Restriction	$\exists r.C$	$German \sqcap \exists worksAt.ITDept$
Universal Restriction	$\forall r.C$	$ITDept \sqcap \forall located.Germany$
Negation	$\neg C$	$\neg German$
(One of) Nominal	$\{a_1, \ldots, a_n\}$	$\{LINDA, JOHN, JIM\}$

$\mathcal{EL}$

- Inexpressive
- Reasoning is in PTime with(out) ontologies

DL Concepts

Name	Syntax	Example
Top	$\top$	*tautology*
Concept Name	A	$Germany$
Conjunction	$C \sqcap D$	$German \sqcap Female$
Disjunction	$C \sqcup D$	$Germany \sqcup Austria$
Existential Restriction	$\exists r.C$	$German \sqcap \exists worksAt.ITDept$
Universal Restriction	$\forall r.C$	$ITDept \sqcap \forall located.Germany$
Negation	$\neg C$	$\neg German$
(One of) Nominal	$\{a_1, \ldots, a_n\}$	$\{LINDA, JOHN, JIM\}$

$\mathcal{FL}_0$

- The dual of $\mathcal{EL}$
- Reasoning is in PTime without ontologies
- Reasoning may be in ExpTime with ontologies

DL Concepts

Name	Syntax	Example
Top	$\top$	*tautology*
Concept Name	A	$Germany$
Conjunction	$C \sqcap D$	$German \sqcap Patient$
Disjunction	$C \sqcup D$	$Germany \sqcup Austria$
Existential Restriction	$\exists r.C$	$German \sqcap \exists worksAt.ITDept$
Universal Restriction	$\forall r.C$	$ITDept \sqcap \forall located.Germany$
Negation	$\neg C$	$\neg German$
(One of) Nominal	$\{a_1, \ldots, a_n\}$	$\{LINDA, JOHN, JIM\}$

$\mathcal{FLE}$

- Combination of $\mathcal{EL}$ and $\mathcal{FL}_0$
- Reasoning is NP-complete without ontologies

DL Ontologies

A **DL ontology** $\mathfrak{O}$ consists of an **ABox** $\mathcal{A}$ and a **TBox** $\mathcal{T}$ $\iff \mathfrak{O} = (\mathcal{T}, \mathcal{A})$

A TBox $\mathcal{T}$: **terminological knowledge**
subsumptions between concepts $C \sqsubseteq D$
(**General Concept Inclusions (GCIs)**)

$\mathcal{T}_1$**:**	$\{\exists seenBy.Oncologist \sqsubseteq \exists suffer.Cancer\}$

DL Ontologies

A **DL ontology** $\mathfrak{O}$ consists of an **ABox** $\mathcal{A}$ and a **TBox** $\mathcal{T}$ $\iff \mathfrak{O} = (\mathcal{T}, \mathcal{A})$

A TBox $\mathcal{T}$: **terminological knowledge**
subsumptions between concepts $C \sqsubseteq D$
(**General Concept Inclusions (GCIs)**)

$\mathcal{T}_1$**:**	$\{\exists seenBy.Oncologist \sqsubseteq \exists suffer.Cancer\}$

An ABox $\mathcal{A}$: **assertional knowledge about individuals**
(instance relationships $C(a)$ and individual relationships $r(a, b)$)

$\mathcal{A}_1$**:**	$\{seenBy(x, PAMELA),\ Oncologist(PAMELA)\}$

Reasoning in Description Logic Ontologies
for Privacy Management

Reasoning in DL Ontologies

$\mathcal{T}_1$: $\{\exists seenBy.Oncologist \sqsubseteq \exists suffer.Cancer\}$

$\mathcal{A}_1$: $\{seenBy(x, PAMELA),\ Oncologist(PAMELA)\}$

What can we infer from $\mathfrak{O}$:

- $\exists seenBy.Oncologist(x) \Rightarrow x$ is seen by an oncologist
- $\exists suffer.Cancer(x) \Rightarrow x$ suffers from a cancer

Prone to Privacy Violations?

$\mathcal{T}_1$: $\{\exists seenBy.Oncologist \sqsubseteq \exists suffer.Cancer\}$

$\mathcal{A}_1$: $\{seenBy(x, PAMELA),\ Oncologist(PAMELA)\}$

What can we infer from $\mathfrak{O}_1 = (\mathcal{T}_1, \mathcal{A}_1)$:

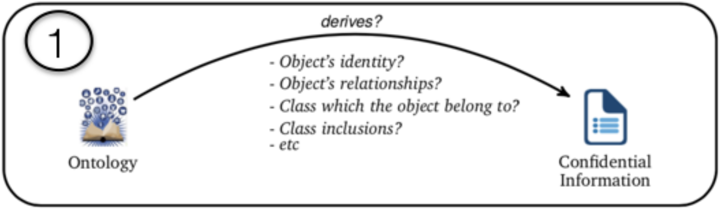
- $\exists seenBy.Oncologist(x) \Rightarrow x$ is seen by an oncologist
- $\exists suffer.Cancer(x) \Rightarrow x$ suffers from a cancer

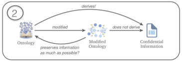
Suppose there is a **privacy policy** P the ontology $\mathfrak{O}_1$ should obey:
It is not allowed to know any disease of any individual of the ontology

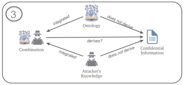
$\mathfrak{O}_1$ does not comply with P

Reasoning in Description Logic Ontologies
for Privacy Management

Anticipation Steps Before Publishing Ontologies

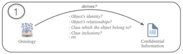


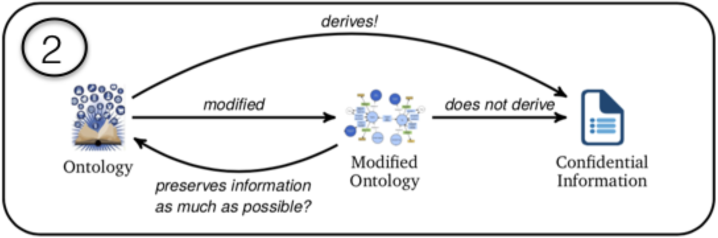


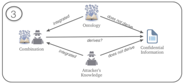


Detect Privacy Breach

Anticipation Steps Before Publishing Ontologies

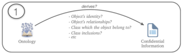


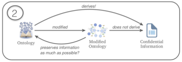


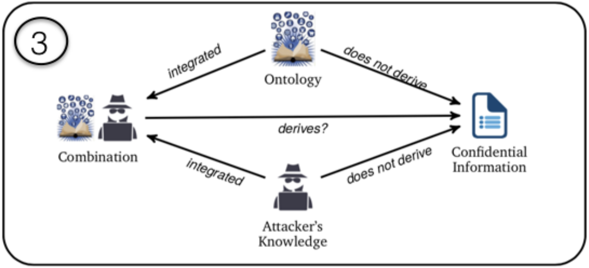


Detect Privacy Breach → Ontology Repair

Anticipation Steps Before Publishing Ontologies







What People Have Done

- Confidential information ⇒ *property of individuals*
- Membership of individuals (tuple of individuals) in the answers to certain queries
  (e.g., **[Calvanesse et. al., 2008]**, **[Stouppa & Studer, 2009]**, **[Tao et.al., 2010]**)

What People Have Done

Detect Privacy Breach → Ontology Repair → Avoid Linkage Attacks

- Confidential information ⇒ *property of individuals*
- Membership of individuals (tuple of individuals) in the answers to certain queries
  (e.g., **[Calvanesse et. al., 2008]**, **[Stouppa & Studer, 2009]**, **[Tao et.al., 2010]**)

Focus on Identity? What is "identity"?

What People Have Done

- Finding justifications why the (unwanted) consequences can be derived (e.g., **[Schlobach, 2003]**, **[Parsia et. al., 2007]**, **[Baader et. al., 2008]**)
- Remove axioms that are responsible for the entailment (e.g., **[Kalyanpur et. al., 2006]**)

What People Have Done

Detect Privacy Breach → **Ontology Repair** → Avoid Linkage Attacks

- Finding justifications why the (unwanted) consequences can be derived (e.g., **[Schlobach, 2003]**, **[Parsia et. al., 2007]**, **[Baader et. al., 2008]**)
- Remove axioms that are responsible for the entailment (e.g., **[Kalyanpur et. al., 2006]**)

Do these approaches also remove useful consequences?
Can we do it more "gentle"?

What People Have Done

- Learning type of attackers' background knowledge
- Investigating *attribute linkage*, *table linkage*, etc thoroughly in e.g., **[Fung et. al., 2010]**
- Introducing the notions of *policy-compliance and policy-safety* in the context of RDF graphs/Linked Data in e.g., **[Grau & Kostylev, 2016]**

What People Have Done

- Learning type of attackers' background knowledge
- Investigating *attribute linkage*, *table linkage*, etc thoroughly in e.g., **[Fung et. al., 2010]**
- Introducing the notions of *policy-compliance and policy-safety* in the context of RDF graphs/Linked Data in e.g., **[Grau & Kostylev, 2016]**

Is such setting already considered in DL ontologies?

Problem Descriptions

Detecting Privacy Breach — The Identity Problem and its Variants in Description Logic Ontologies

Ontology Repair — Repairing Description Logic Ontologies via Axiom Weakening

Avoiding Linkage Attacks — Privacy-Preserving Ontology Publishing

Discussed in **[Nuradiansyah, 2019]**

Problem 1: Is My Identity Safe?

An ontology $\mathfrak{O}_2 = (\mathcal{T}_2, \mathcal{A}_2)$ extends the ontology $\mathfrak{O}_1$ as follows:

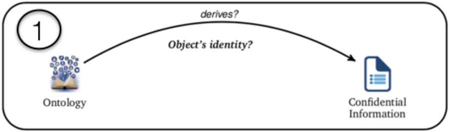
$$\mathcal{T}_2\textbf{:} \quad \{\exists seenBy.Oncologist \sqsubseteq \exists suffer.Cancer, \exists suffer.Cancer \equiv \{LINDA, BOB\}, Female \sqsubseteq \neg MALE\}$$

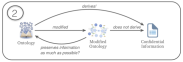
$$\mathcal{A}_2\textbf{:} \quad \{seenBy(x, PAMELA), \; Oncologist(PAMELA), Male(BOB), Male(x), Female(LINDA)\}$$

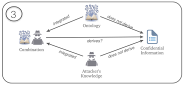
What we can infer from $\mathfrak{O}_2$:

- x suffers from Cancer
- the only male known individual who suffers from cancer is Bob
- x is Bob!

Problem 1: The Identity Problem

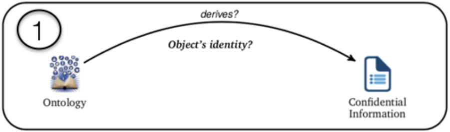


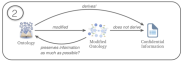


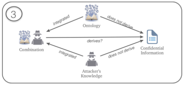


Identity Problem ($\mathcal{O} \models x \doteq a$) [DL 2017], [JIST 2017]

Problem 1: The Identity Problem



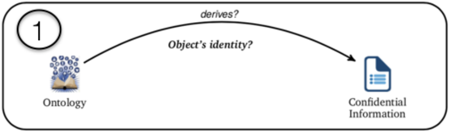


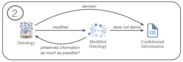


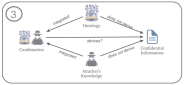
Identity Problem ($\mathcal{O} \models x \doteq a$) [DL 2017], [JIST 2017]

- Not all DLs are able to derive equalities between individuals, e.g. $\mathcal{ALC}$.
- **DLs with equality power**: nominals, number restrictions, and functional dependencies.

Problem 1: The Identity Problem







Identity Problem ($\mathfrak{O} \models x \doteq a$) [DL 2017], [JIST 2017]

- Not all DLs are able to derive equalities between individuals, e.g. $\mathcal{ALC}$.
- **DLs with equality power**: nominals, number restrictions, and functional dependencies.
- **Identity to Instance**: Given two individuals x, a, and an ontology $\mathfrak{O}$ formulated in a DL with equality power, it holds

$$\mathfrak{O} \models x \doteq a \text{ iff } (\mathfrak{O} \cup \{Q(x)\}) \models Q(a), \text{ where } Q \text{ is a fresh concept name}$$

Given an ontology $\mathfrak{O}_I$

At role $\hat{r}_1$
- queries through $\mathfrak{O}_{r_1} \subseteq \mathfrak{O}_I$
- obtains View V_{r_1}

$\xrightarrow{\text{switch}} \cdots \xrightarrow{\text{switch}}$

At role $\hat{r}_k$
- queries through $\mathfrak{O}_{r_k} \subseteq \mathfrak{O}_I$
- obtains View V_{r_k}

Is the identity of an anonymous x hidden w.r.t. $V_{\hat{r}_1}, \ldots, V_{\hat{r}_k}$?

(**The View-Based Identity (VBI) Problem**)

The Identity Problem in Role-Based Access Control

Given an ontology $\mathfrak{O}_I$

At role $\hat{r}_1$

- queries through $\mathfrak{O}_{r_1} \subseteq \mathfrak{O}_I$
- obtains View V_{r_1}

$\xrightarrow{\text{switch}} \cdots \xrightarrow{\text{switch}}$

At role $\hat{r}_k$

- queries through $\mathfrak{O}_{r_k} \subseteq \mathfrak{O}_I$
- obtains View V_{r_k}

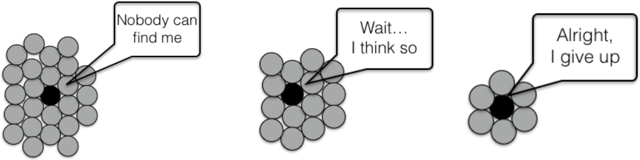
Is the identity of an anonymous x hidden w.r.t. $V_{\hat{r}_1}, \ldots, V_{\hat{r}_k}$?

(**The View-Based Identity (VBI) Problem**)

Reduction

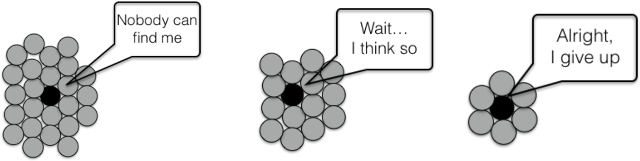
The VBI problem can be reduced to the identity problem for *some* DLs with equality power

Hiding in the Middle of k Known Individuals



"Hiding in the crowd" ...

Hiding in the Middle of k Known Individuals



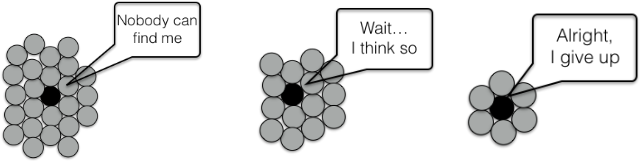
"Hiding in the crowd" ...

The k-Hiding Problem

The anonymous individual x is **not k-hidden** w.r.t. $\mathfrak{O}$ iff there are known individuals $a_1, \ldots, a_{k-1}$ such that

$$x \text{ belongs to } \{a_1, \ldots, a_{k-1}\} \text{ w.r.t. } \mathfrak{O}$$

Hiding in the Middle of k Known Individuals



"Hiding in the crowd" ...

The k-Hiding Problem

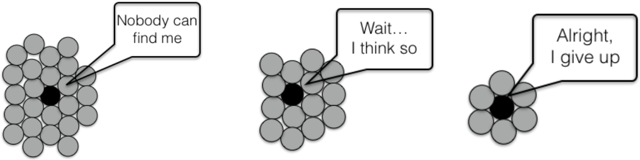
The anonymous individual x is **not k-hidden** w.r.t. $\mathfrak{O}$ iff there are known individuals $a_1, \ldots, a_{k-1}$ such that

$$x \text{ belongs to } \{a_1, \ldots, a_{k-1}\} \text{ w.r.t. } \mathfrak{O}$$

How to solve it

- Reduce it to the instance problem for *all* DLs with equality power
- Reduce it to the identity problem for *some* convex DLs with equality power

Hiding in the Middle of k Known Individuals



"Hiding in the crowd" ...

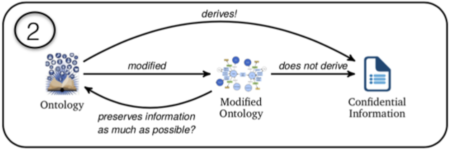
The k-Hiding Problem

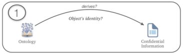
The anonymous individual x is **not k-hidden** w.r.t. $\mathfrak{O}$ iff there are known individuals $a_1, \ldots, a_{k-1}$ such that

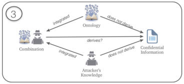
$$x \text{ belongs to } \{a_1, \ldots, a_{k-1}\} \text{ w.r.t. } \mathfrak{O}$$

*If (variants) of the identity problem can be reduced to classical reasoning problems in DLs, then now let's consider **more general types of confidential axioms** (e.g., instance relationships, subsumptions, CQs, etc).*

Problem 2: How to Protect the Confidential Information?







Ontology Repair ([KR 2018])

- Given an (secret) axiom α such that an ontology $\mathfrak{O}$ entails α
- An ontology $\mathfrak{O}'$ is a **repair** of $\mathfrak{O}$ w.r.t. α if
  - $\mathfrak{O}' \not\models \alpha$
  - $\mathfrak{O} \models \mathfrak{O}'$
- Such a repair is **optimal** if there is no repair $\mathfrak{O}''$ that strictly implies $\mathfrak{O}'$.

Optimal Classical Repairs

Optimal Repairs need not exist in general!

Optimal Classical Repair

A maximum subset $\mathfrak{O}'$ of $\mathfrak{O}$ such that $\mathfrak{O}' \not\models \alpha$

Optimal Classical Repairs

Optimal Repairs need not exist in general!

Optimal Classical Repair

A maximum subset $\mathfrak{O}'$ of $\mathfrak{O}$ such that $\mathfrak{O}' \not\models \alpha$

- Optimal classical repairs always exist $\rightarrow$ **Justification** and **Hitting Set** **(Reiter, 1987)**

Optimal Classical Repairs

Optimal Repairs need not exist in general!

Optimal Classical Repair

A maximum subset $\mathfrak{O}'$ of $\mathfrak{O}$ such that $\mathfrak{O}' \not\models \alpha$

- Optimal classical repairs always exist $\rightarrow$ **Justification** and **Hitting Set** **(Reiter, 1987)**
- **Justification** $J \Rightarrow$ a minimum subset of $\mathfrak{O}$ w.r.t. α such that $J \models \alpha$
- **Hitting set** $H \Rightarrow$ taking one element from each justification of $\mathfrak{O}$ w.r.t. α
- Only consider a minimal hitting set H_{min}
- $\mathfrak{O}' := \mathfrak{O} \setminus H_{min}$ is an optimal classical repair

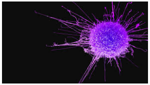
Gentle Repair

Obtaining Classical Repairs → **removing axioms** from $\mathfrak{O}$.

Instead, we want to **weaken axioms** in $\mathcal{H}$ ⇒ **Gentle Repair**!

Given axioms β, γ, an axiom γ is **weaker than** β if $Con(\{\gamma\}) \subset Con(\{\beta\})$

Illustration

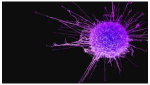


Gentle Repair

Illustration

$$\mathfrak{O}_3 := \{\exists seenBy.(Doctor \sqcap \exists worksIn.Oncology) \sqsubseteq \exists suffer.Cancer,$$
$$\exists worksIn.Nuclear \sqsubseteq \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology),$$
$$\exists worksIn.Nuclear(LINDA)\}$$

- $\mathfrak{O}_3$ does not comply with $\mathcal{P}$
- Suppose we are only allowed to modify the second axiom

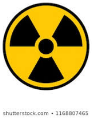


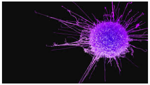
Gentle Repair

Illustration

$$\mathfrak{O}_3 := \{\, \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology) \sqsubseteq \exists suffer.Cancer,$$
$$\exists worksIn.Nuclear \sqsubseteq \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology),$$
$$\exists worksIn.Nuclear(LINDA)\,\}$$

- $\mathfrak{O}_3$ does not comply with $\mathcal{P}$
- Suppose we are only allowed to modify the second axiom
- **Classical:** Remove the second axiom entirely
  Assume that some parts of the second axiom are useful to be retained





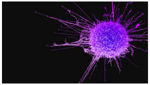
Gentle Repair

Illustration

$$\mathfrak{O}_3 := \{\exists seenBy.(Doctor \sqcap \exists worksIn.Oncology) \sqsubseteq \exists suffer.Cancer, \\ \exists worksIn.Nuclear \sqsubseteq \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology), \\ \exists worksIn.Nuclear(LINDA)\}$$

- $\mathfrak{O}_3$ does not comply with $\mathcal{P}$
- Suppose we are only allowed to modify the second axiom
- **Gentle**: Weaken the second axiom to

$$\exists worksIn.Nuclear \sqsubseteq \exists seenBy.Doctor \sqcap \\ \exists seenBy.\exists worksIn.Oncology$$



How to Make it Gentle?

Gentle Repair Algorithm: **[KR 2018]**

- Take all justifications and one minimal hitting set $\mathcal{H}_{min}$

How to Make it Gentle?

Gentle Repair Algorithm: **[KR 2018]**

- Take all justifications and one minimal hitting set $\mathcal{H}_{min}$
- For each $\beta \in \mathcal{H}_{min}$ and all $J_1, \ldots, J_k$ containing β,

How to Make it Gentle?

Gentle Repair Algorithm: **[KR 2018]**

- Take all justifications and one minimal hitting set $\mathcal{H}_{min}$
- For each $\beta \in \mathcal{H}_{min}$ and all $J_1, \ldots, J_k$ containing β, **replace** β with **exactly one** γ, where γ is weaker than β such that

$$\mathfrak{O}_s \cup (J_i \setminus \{\beta\}) \cup \{\gamma\} \not\models \alpha \text{ for } i = 1, \ldots, k. \quad (1)$$

γ always exists.

How to Make it Gentle?

Gentle Repair Algorithm: **[KR 2018]**

- Take all justifications and one minimal hitting set $\mathcal{H}_{min}$
- For each $\beta \in \mathcal{H}_{min}$ and all $J_1, \ldots, J_k$ containing β, **replace** β with **exactly one** γ, where γ is weaker than β such that

$$\mathfrak{O}_s \cup (J_i \setminus \{\beta\}) \cup \{\gamma\} \not\models \alpha \text{ for } i = 1, \ldots, k. \quad (1)$$

  γ always exists.

- **Construct** $\mathfrak{O}$' **obtained** from $\mathfrak{O}_r$ by **replacing** each $\beta \in \mathcal{H}_{min}$ with an appropriate weaker γ satisfying (1).

How to Make it Gentle?

Gentle Repair Algorithm: **[KR 2018]**

- Take all justifications and one minimal hitting set $\mathcal{H}_{min}$
- For each $\beta \in \mathcal{H}_{min}$ and all $J_1, \ldots, J_k$ containing β, **replace** β with **exactly one** γ, where γ is weaker than β such that

$$\mathfrak{O}_s \cup (J_i \setminus \{\beta\}) \cup \{\gamma\} \not\models \alpha \text{ for } i = 1, \ldots, k. \quad (1)$$

  γ always exists.

- **Construct** $\mathfrak{O}$' **obtained** from $\mathfrak{O}_r$ by **replacing** each $\beta \in \mathcal{H}_{min}$ with an appropriate weaker γ satisfying (1).
- **Check** if α is a consequence of $\mathfrak{O}'$.

How to Make it Gentle?

Gentle Repair Algorithm: **[KR 2018]**

- Take all justifications and one minimal hitting set $\mathcal{H}_{min}$
- For each $\beta \in \mathcal{H}_{min}$ and all $J_1, \ldots, J_k$ containing β, **replace** β with **exactly one** γ, where γ is weaker than β such that

$$\mathfrak{O}_s \cup (J_i \setminus \{\beta\}) \cup \{\gamma\} \not\models \alpha \text{ for } i = 1, \ldots, k. \quad (1)$$

  γ always exists.

- **Construct** $\mathfrak{O}$' **obtained** from $\mathfrak{O}_r$ by **replacing** each $\beta \in \mathcal{H}_{min}$ with an appropriate weaker γ satisfying (1).
- **Check** if α is a consequence of $\mathfrak{O}'$.

Obtaining Gentle Repairs needs Iterations

- Using the algorithm above, α still can be a consequence of $\mathfrak{O}'$.
- Solution: Just **iterate** Gentle Repair Algorithm until $\mathfrak{O}' \not\models \alpha$.
- The iterative algorithm yields **an exponential upper bound** on the number of iterations.

Weakening Relations

To obtain **better number of iterations** and to **guide** us when weakening axioms, we introduce **weakening relations** $\succ$ on axioms.

For each $(\beta, \gamma) \in \succ$, γ is weaker than β

Weakening Relations

To obtain **better number of iterations** and to **guide** us when weakening axioms, we introduce **weakening relations** $\succ$ on axioms.

For each $(\beta, \gamma) \in \succ$, γ is weaker than β

Weakening relations provide us (in)finite weakening chains

$$\beta \succ \beta_1 \succ \beta_2 \succ \beta_3 \succ \dots$$

Weakening Relations

To obtain **better number of iterations** and to **guide** us when weakening axioms, we introduce **weakening relations** $\succ$ on axioms.

For each $(\beta, \gamma) \in \succ$, γ is weaker than β

Weakening relations provide us (in)finite weakening chains

$$\beta \succ \beta_1 \succ \beta_2 \succ \beta_3 \succ \dots$$

Weakening relations making **larger steps** may **decrease** the number of iterations

Weakening relations making **smaller steps** may make the repair more gentle

Maximally Strong Weakening Axioms

Replace β with exactly one weaker γ s.t.

$$(J_i \setminus \{\beta\}) \cup \{\gamma\} \not\models \alpha \text{ for } i = 1, \ldots, k$$

If γ is a tautology, then it is **the same as** classical repair.

Maximally Strong Weakening Axioms

Replace β with exactly one weaker γ s.t.

$$(J_i \setminus \{\beta\}) \cup \{\gamma\} \not\models \alpha \text{ for } i = 1, \ldots, k$$

If γ is a tautology, then it is **the same as** classical repair.

To make this repair as gentle as possible, γ should be **maximally strong**

$$(J_i \setminus \{\beta\}) \cup \{\gamma\} \not\models \alpha$$

but for all δ such that $\beta \succ \delta \succ \gamma$, we have

$$(J_i \setminus \{\beta\}) \cup \{\delta\} \models \alpha$$

Maximally Strong Weakening Axioms

Replace β with exactly one weaker γ s.t.

$$(J_i \setminus \{\beta\}) \cup \{\gamma\} \not\models \alpha \text{ for } i = 1, \ldots, k$$

If γ is a tautology, then it is **the same as** classical repair.

To make this repair as gentle as possible, γ should be **maximally strong**

$$(J_i \setminus \{\beta\}) \cup \{\gamma\} \not\models \alpha$$

but for all δ such that $\beta \succ \delta \succ \gamma$, we have

$$(J_i \setminus \{\beta\}) \cup \{\delta\} \models \alpha$$

Do they always exists?

How to compute them?

Weakening Relations in $\mathcal{EL}$

Focus on GCIs and generalize the right-hand side of GCIs.

A Weakening Relation $\succ^{sub}$

$C \sqsubseteq D \succ^{sub} C' \sqsubseteq D'$ if $C' = C,\ D \sqsubset D'$, and
$\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D$.

$D \sqsubset^{syn} D' \Rightarrow$ removing occurrences of subconcepts of D.

A Weakening Relation $\succ^{syn}$

$C \sqsubseteq D \succ^{syn} C' \sqsubseteq D'$ if $C' = C$ and $D \sqsubset^{syn} D'$, and
$\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D$.

Weakening Relations in $\mathcal{EL}$

Focus on GCIs and generalize the right-hand side of GCIs.

A Weakening Relation $\succ^{sub}$

$C \sqsubseteq D \succ^{sub} C' \sqsubseteq D'$ if $C' = C,\ D \sqsubset D'$, and $\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D$.

- $\succ^{sub}$-weakening chains are not polynomial
- $\mid D' \mid$ can be exponentially bounded by $\mid D \mid$

$D \sqsubset^{syn} D' \Rightarrow$ removing occurrences of subconcepts of D.

A Weakening Relation $\succ^{syn}$

$C \sqsubseteq D \succ^{syn} C' \sqsubseteq D'$ if $C' = C$ and $D \sqsubset^{syn} D'$, and $\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D$.

Weakening Relations in $\mathcal{EL}$

Focus on GCIs and generalize the right-hand side of GCIs.

A Weakening Relation $\succ^{sub}$

$C \sqsubseteq D \succ^{sub} C' \sqsubseteq D'$ if $C' = C,\ D \sqsubset D'$, and
$\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D$.

$$\exists worksIn.Nuclear \sqsubseteq \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology)$$
$$\succ^{sub}$$
$$\exists worksIn.Nuclear \sqsubseteq \exists seenBy.Doctor \sqcap \exists seenBy.\exists worksIn.Oncology$$

$D \sqsubset^{syn} D' \Rightarrow$ removing occurrences of subconcepts of D.

A Weakening Relation $\succ^{syn}$

$C \sqsubseteq D \succ^{syn} C' \sqsubseteq D'$ if $C' = C$ and $D \sqsubset^{syn} D'$, and
$\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D$.

Weakening Relations in $\mathcal{EL}$

Focus on GCIs and generalize the right-hand side of GCIs.

A Weakening Relation $\succ^{sub}$

$C \sqsubseteq D \succ^{sub} C' \sqsubseteq D'$ if $C' = C,\ D \sqsubset D'$, and
$\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D$.

- $\succ^{syn}$-weakening chains are linear ($| D | > | D' |$)
- Computing an (all) MSW(s) can be done in polynomial (exponential) time w.r.t. $\succ^{syn}$

$D \sqsubset^{syn} D' \Rightarrow$ removing occurrences of subconcepts of D.

A Weakening Relation $\succ^{syn}$

$C \sqsubseteq D \succ^{syn} C' \sqsubseteq D'$ if $C' = C$ and $D \sqsubset^{syn} D'$, and
$\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D$.

Weakening Relations in $\mathcal{EL}$

Focus on GCIs and generalize the right-hand side of GCIs.

A Weakening Relation $\succ^{sub}$

$C \sqsubseteq D \succ^{sub} C' \sqsubseteq D'$ if $C' = C, \; D \sqsubset D'$, and
$\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D$.

$$\exists worksIn.Nuclear \sqsubseteq \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology)$$
$$\succ^{syn}$$
$$\exists worksIn.Nuclear \sqsubseteq \exists seenBy.Doctor$$

$D \sqsubset^{syn} D' \Rightarrow$ removing occurrences of subconcepts of D.

A Weakening Relation $\succ^{syn}$

$C \sqsubseteq D \succ^{syn} C' \sqsubseteq D'$ if $C' = C$ and $D \sqsubset^{syn} D'$, and
$\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D$.

Weakening Relations in $\mathcal{EL}$

Focus on GCIs and generalize the right-hand side of GCIs.

A Weakening Relation $\succ^{sub}$

$C \sqsubseteq D \succ^{sub} C' \sqsubseteq D'$ if $C' = C,\ D \sqsubset D'$, and
$$\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D.$$

or $\exists worksIn.Nuclear \sqsubseteq \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology)$
$$\succ^{syn}$$
$$\exists worksIn.Nuclear \sqsubseteq \exists seenBy.\exists worksIn.Oncology$$

$D \sqsubset^{syn} D' \Rightarrow$ removing occurrences of subconcepts of D.

A Weakening Relation $\succ^{syn}$

$C \sqsubseteq D \succ^{syn} C' \sqsubseteq D'$ if $C' = C$ and $D \sqsubset^{syn} D'$, and
$$\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D.$$

Weakening Relations in $\mathcal{EL}$

Focus on GCIs and generalize the right-hand side of GCIs.

A Weakening Relation $\succ^{sub}$

$C \sqsubseteq D \succ^{sub} C' \sqsubseteq D'$ if $C' = C,\ D \sqsubset D'$, and
$$\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D.$$

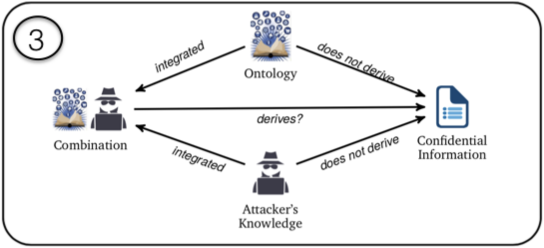
Employing both, maximally strong weakenings can be effectively computed

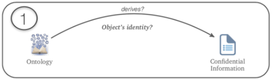
$D \sqsubset^{syn} D' \Rightarrow$ removing occurrences of subconcepts of D.

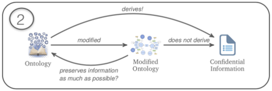
A Weakening Relation $\succ^{syn}$

$C \sqsubseteq D \succ^{syn} C' \sqsubseteq D'$ if $C' = C$ and $D \sqsubset^{syn} D'$, and
$$\{C' \sqsubseteq D'\} \not\models C \sqsubseteq D.$$

Problem 3: Privacy-Preserving Ontology Publishing (PPOP)







PPOP for $\mathcal{EL}$ Ontologies ([DL 2018], [JELIA 2019], [KI 2019])

Restricting the ontology:

- Instance Stores & ABoxes (**No TBoxes**)
- **Instance Stores**: Ontologies without individual relationships

$\mathcal{EL}$ Instance Stores without TBox

$C_1(a), C_2(a)$ implies $(C_1 \sqcap C_2)(a)$

only one concept assertion speaking about one individual

Published Information

(an $\mathcal{EL}$ Concept C)

Attacker's Knowledge

(an $\mathcal{EL}$ / $\mathcal{FL}_0$ / $\mathcal{FLE}$ Concept E)

Confidential Information

(a finite set of $\mathcal{EL}$ concepts) $\{D_1, \ldots, D_p\}$

Privacy Attacks in $\mathcal{EL}$ Instance Stores

Confidential Information $\mathcal{P} = \{D\}$ about *LINDA*

$$D = Patient \sqcap \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology)$$

Original **Published Information** C about *LINDA*

$$C = Patient \sqcap Female \sqcap \exists seenBy.(Doctor \sqcap Male \sqcap \exists worksIn.Oncology)$$

Note C is not **compliant with** D

Privacy Attacks in $\mathcal{EL}$ Instance Stores

Confidential Information $\mathcal{P} = \{D\}$ about *LINDA*

$$D = Patient \sqcap \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology)$$

Original **Published Information** C about *LINDA*

$$C = Patient \sqcap Female \sqcap \exists seenBy.(Doctor \sqcap Male \sqcap \exists worksIn.Oncology)$$

Note C is not **compliant with** D

Modification

$$C_1 = Female \sqcap \exists seenBy.(Doctor \sqcap Male \sqcap \exists worksIn.Oncology)$$

Note $C \sqsubseteq C_1$ and C_1 **complies with** D

Confidential Information $\mathcal{P} = \{D\}$ about *LINDA*

$$D = Patient \sqcap \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology)$$

Original **Published Information** C about *LINDA*

$$C = Patient \sqcap Female \sqcap \exists seenBy.(Doctor \sqcap Male \sqcap \exists worksIn.Oncology)$$

Note C is not **compliant with** D

$\mathcal{EL}$**-Attacker is Coming!**

$$C_1 = Female \sqcap \exists seenBy.(Doctor \sqcap Male \sqcap \exists worksIn.Oncology)$$

He knows $\{Patient(LINDA)\}$ is **compliant with** D

Privacy Attacks in $\mathcal{EL}$ Instance Stores

Confidential Information $\mathcal{P} = \{D\}$ about *LINDA*

$$D = Patient \sqcap \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology)$$

Original **Published Information** C about *LINDA*

$$C = Patient \sqcap Female \sqcap \exists seenBy.(Doctor \sqcap Male \sqcap \exists worksIn.Oncology)$$

Note C is not **compliant with** D

Linked and Revealed!

$$C_1' = Female \sqcap \exists seenBy.(Doctor \sqcap Male \sqcap \exists worksIn.Oncology) \sqcap \textbf{Patient}$$

Note $D(LINDA)$ is **revealed** and C_1 is not $\mathcal{EL}$-safe for D

Privacy Attacks in $\mathcal{EL}$ Instance Stores

Confidential Information $\mathcal{P} = \{D\}$ about *LINDA*

$$D = Patient \sqcap \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology)$$

Original **Published Information** C about *LINDA*

$$C = Patient \sqcap Female \sqcap \exists seenBy.(Doctor \sqcap Male \sqcap \exists worksIn.Oncology)$$

Note C is not **compliant with** D

Modification

$$C_2 = Female \sqcap \exists seenBy.(Doctor \sqcap Male \sqcap \exists worksIn.\top)$$

C_2 is $\mathcal{EL}$**-safe** for D

Privacy Attacks in $\mathcal{EL}$ Instance Stores

Confidential Information $\mathcal{P} = \{D\}$ about *LINDA*

$$D = Patient \sqcap \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology)$$

Original **Published Information** C about *LINDA*

$$C = Patient \sqcap Female \sqcap \exists seenBy.(Doctor \sqcap Male \sqcap \exists worksIn.Oncology)$$

Note C is not **compliant with** D

Modification

$$C_2 = Female \sqcap \exists seenBy.(Doctor \sqcap Male \sqcap \exists worksIn.\top)$$

Every top-level conjunct in D has no subsumee that becomes a top-level conjunct in C_2

Privacy Attacks in $\mathcal{EL}$ Instance Stores

Confidential Information $\mathcal{P} = \{D\}$ about *LINDA*

$$D = Patient \sqcap \exists seenBy.(Doctor \sqcap \exists worksIn.Oncology)$$

Original **Published Information** C about *LINDA*

$$C = Patient \sqcap Female \sqcap \exists seenBy.(Doctor \sqcap Male \sqcap \exists worksIn.Oncology)$$

Note C is not **compliant with** D

Modification

$$C_2 = Female \sqcap \exists seenBy.(Doctor \sqcap Male \sqcap \exists worksIn.\top) \sqcap \exists seenBy.(Male \sqcap worksIn.Oncology)$$

C_2 is the optimal $\mathcal{EL}$-**safe** generalization of C for D

Decision & Computational Problems on PPOP for $\mathcal{EL}$ Instance Stores

Given $\mathcal{L} \in \{\mathcal{EL}, \mathcal{FL}_0, \mathcal{FLE}\}$, a published information ($\mathcal{EL}$ concept) C, an $\mathcal{EL}$ confidential information $\mathcal{P}$.

Decision Problem

$\mathcal{L}$-Optimality:
Is an $\mathcal{EL}$ concept C_1 an optimal $\mathcal{L}$-safe generalization of C for $\mathcal{P}$?

Computational Problem

Find an $\mathcal{EL}$ concept C_1 s.t C_1 is an optimal $\mathcal{L}$-safe generalization of C for $\mathcal{P}$!

Complexity Results on PPOP for $\mathcal{EL}$ Instance Stores

All results are written in [JELIA2019] and [KI2019]

Decision Problems	$\mathcal{L} = \mathcal{EL}$	$\mathcal{L} = \mathcal{FL}_0$	$\mathcal{L} = \mathcal{FLE}$
$\mathcal{L}$-optimality	coNP and Dual-hard	coNP and Dual-hard	PTime

Table: Complexity results of $\mathcal{L}$-optimality on PPOP for $\mathcal{EL}$ instance stores

Computational Problems	$\mathcal{L} = \mathcal{EL}$	$\mathcal{L} = \mathcal{FL}_0$	$\mathcal{L} = \mathcal{FLE}$
Optimal $\mathcal{L}$-safe Generalization(s)	ExpTime	ExpTime	PTime

Table: Complexity of computing one/all optimal Q-safe generalizations for $\mathcal{P}$

The stronger the capability of the attacker, concepts need to be changed more radically

PPOP for $\mathcal{EL}$ ABoxes

Including relationships between individuals in $\mathcal{EL}$ ABoxes.

Published Information
(an $\mathcal{EL}$ ABox)

Attacker's Knowledge
(an $\mathcal{EL}$ ABox)

Confidential Information
(an instance query ($\mathcal{EL}$ concept) or **a conjunctive query)**

PPOP for $\mathcal{EL}$ ABoxes

Including relationships between individuals in $\mathcal{EL}$ ABoxes.

Published Information
(an $\mathcal{EL}$ ABox)

Attacker's Knowledge
(an $\mathcal{EL}$ ABox)

Confidential Information
(an instance query ($\mathcal{EL}$ concept) or **a conjunctive query)**

A **conjunctive query** q: $\exists \vec{w}.conj(\vec{v}, \vec{w})$, where
$conj(\vec{v}, \vec{w})$ is a conjunction of unary or binary predicates over variables $\vec{v} \cup \vec{w}$

A sort of `SELECT-JOIN-PROJECT` query in DBs

Confidential Information D for each individual

$$D = Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood) \sqcap \exists seenBy.Oncologist$$

Original **Published Information** $\mathcal{A}$

$$\mathcal{A} = \{seenBy(LINDA, JOHN), Male \sqcap Oncologist(JOHN), Female \sqcap Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood)(LINDA)\}$$

Note $\mathcal{A}$ is not **compliant with** D

Privacy Attacks in $\mathcal{EL}$ ABoxes

Confidential Information D for each individual

$$D = Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood) \sqcap \exists seenBy.Oncologist$$

Original **Published Information** $\mathcal{A}$

$$\mathcal{A} = \{seenBy(LINDA, JOHN), Male \sqcap Oncologist(JOHN), \\ Female \sqcap Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood)(LINDA)\}$$

Note $\mathcal{A}$ is not **compliant with** D

Modification

$$\mathcal{A}_1 = \{seenBy(LINDA, x), Male \sqcap Oncologist(y), \\ Female \sqcap Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood)(LINDA)\}$$

$\mathcal{A}_1$ **complies with** D

Privacy Attacks in $\mathcal{EL}$ ABoxes

Confidential Information D for each individual

$$D = Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood) \sqcap \exists seenBy.Oncologist$$

Original **Published Information** $\mathcal{A}$

$$\mathcal{A} = \{seenBy(LINDA, JOHN), Male \sqcap Oncologist(JOHN), \\ Female \sqcap Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood)(LINDA)\}$$

Note $\mathcal{A}$ is not **compliant with** D

An Attacker is Coming!

$$\mathcal{A}_1 = \{seenBy(LINDA, x), Male \sqcap Oncologist(y), \\ Female \sqcap Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood)(LINDA)\}$$

He **knows** $\{seenBy(LINDA, JOHN), Male \sqcap Oncologist(JOHN)\}$ is compliant with D

Privacy Attacks in $\mathcal{EL}$ ABoxes

Confidential Information D for each individual

$$D = Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood) \sqcap \exists seenBy.Oncologist$$

Original **Published Information** $\mathcal{A}$

$$\mathcal{A} = \{seenBy(LINDA, JOHN), Male \sqcap Oncologist(JOHN),$$
$$Female \sqcap Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood)(LINDA)\}$$

Note $\mathcal{A}$ is not **compliant with** D

Combination of $\mathcal{A}_1$ and the attacker's knowledge **reveals** $D(LINDA)$

Privacy Attacks in $\mathcal{EL}$ ABoxes

Confidential Information D for each individual

$$D = Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood) \sqcap \exists seenBy.Oncologist$$

Original **Published Information** $\mathcal{A}$

$$\mathcal{A} = \{seenBy(LINDA, JOHN), Male \sqcap Oncologist(JOHN),$$
$$Female \sqcap Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood)(LINDA)\}$$

Note $\mathcal{A}$ is not **compliant with** D

Modification

$$\mathcal{A}_2 = \{seenBy(LINDA, x), Male(JOHN),$$
$$Female \sqcap \exists suffer.\exists attack.Blood(LINDA)\}$$

$\mathcal{A}_2$ **is safe for** D

Privacy Attacks in $\mathcal{EL}$ ABoxes

Confidential Information D for each individual

$$D = Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood) \sqcap \exists seenBy.Oncologist$$

Original **Published Information** $\mathcal{A}$

$$\mathcal{A} = \{seenBy(LINDA, JOHN), Male \sqcap Oncologist(JOHN),$$
$$Female \sqcap Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood)(LINDA)\}$$

Note $\mathcal{A}$ is not **compliant with** D

Modification

$$\mathcal{A}_2 = \{seenBy(LINDA, x), Male(JOHN),$$
$$Female \sqcap \exists suffer.\exists attack.Blood(LINDA)\}$$

No top-level conjunct in D that has "implicit" subsumee in $\mathcal{A}_2$

Privacy Attacks in $\mathcal{EL}$ ABoxes

Confidential Information D for each individual

$$D = Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood) \sqcap \exists seenBy.Oncologist$$

Original **Published Information** $\mathcal{A}$

$$\mathcal{A} = \{seenBy(LINDA, JOHN), Male \sqcap Oncologist(JOHN), Female \sqcap Patient \sqcap \exists suffer.(Cancer \sqcap \exists attack.Blood)(LINDA)\}$$

Note $\mathcal{A}$ is not **compliant with** D

Modification

$$\mathcal{A}_3 = \{seenBy(LINDA, x), Male(JOHN), Female \sqcap \exists suffer.Cancer \sqcap \exists suffer.\exists attack.Blood(LINDA)\}$$

$\mathcal{A}_3$ **is safe for** D and more "optimal" than $\mathcal{A}_2$

Anonymizing EL ABoxes

How to modify $\mathcal{EL}$ ABoxes?

$\mathcal{A}$ $\xrightarrow{\mathcal{A}\text{-anonymizer f}}$ $\mathcal{A}$

1. Replace individuals with new anonymous individuals

2. Two different individuals cannot be replaced by the same anonymous individual

3. Generalizing concepts

$\mathcal{A}$ **$\mathcal{A}$-anonymizer f** $\longrightarrow$ $\mathcal{A}$

1. Replace individuals with new anonymous individuals

2. Two different individuals cannot be replaced by the same anonymous individual

3. Generalizing concepts

Measuring Optimality

An $\mathcal{A}$-anonymizer f_2 is **more informative than** an $\mathcal{A}$-anonymizer f_1 ($f_2 > f_1$) if f_2 can be obtained from f_1 by:

- keeping more known individuals
- identifying more distinct anonymous individuals
- specializing more $\mathcal{EL}$ concepts

Decision Problems on PPOP for $\mathcal{EL}$ ABoxes

Given an $\mathcal{EL}$ ABox $\mathcal{A}$, an $\mathcal{EL}$ concept D, and an $\mathcal{A}$-anonymizer f, we consider the decision problems

- **Safety$_C$**: is $\mathcal{A}$ safe for D? and
- **Optimal-Safety$_C$** which asks
  - if $f(\mathcal{A})$ is safe for D and
  - for all $\mathcal{A}$-anonymizers f', if $f' > f$, then $f'(\mathcal{A})$ is not safe for D

Analogous to **Safety$_{CQ}$** and **Optimal-Safety$_{CQ}$**, where the policy is a CQ

Decision Problems on PPOP for $\mathcal{EL}$ ABoxes

Given an $\mathcal{EL}$ ABox $\mathcal{A}$, an $\mathcal{EL}$ concept D, and an $\mathcal{A}$-anonymizer f, we consider the decision problems

- **Safety$_C$**: is $\mathcal{A}$ safe for D? and
- **Optimal-Safety$_C$** which asks
  - if $f(\mathcal{A})$ is safe for D and
  - for all $\mathcal{A}$-anonymizers f', if $f' > f$, then $f'(\mathcal{A})$ is not safe for D

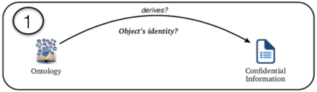
Analogous to **Safety$_{CQ}$** and **Optimal-Safety$_{CQ}$**, where the policy is a CQ

Decision Problems	**X = C**	**X = CQ**
Safety$_X$	PTime	Π_2^p and DP-hard
Optimal-Safety$_X$	coNP and Dual-hard	Π_3^p and DP-hard

Conclusions

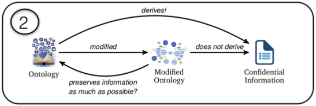
The Identity Problem:

- Non trivial for DLs with equality power
- Introducing variants of the identity problem
- Reduction to classical reasoning in DLs



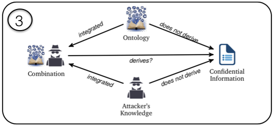
Gentle Repair:

- Introducing a framework for repair via axiom weakening
- Weakening relations
- Weakening axioms in $\mathcal{EL}$



Privacy-Preserving Ontology Publishing:

- PPOP for $\mathcal{EL}$ Instance Stores
- PPOP for $\mathcal{EL}$ ABoxes
- Applying the notions of safety and optimality in both settings

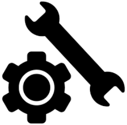


Future Work

1. Adding **probabilistic axioms** into ontologies
   - Equalities between individual hold with certain probabilistic values
2. Considering **heuristic** approaches to make ontology repairs more gentle
   - Which axiom needs to be weaken first
   - Which axiom that is more suitable to be chosen as a maximally strong weakening axiom

Future Work

1. Adding **probabilistic axioms** into ontologies
   - Equalities between individual hold with certain probabilistic values
2. Considering **heuristic** approaches to make ontology repairs more gentle
   - Which axiom needs to be weaken first
   - Which axiom that is more suitable to be chosen as a maximally strong weakening axiom
3. Extending the setting of PPOP in $\mathcal{EL}$ Ontologies
   - Considering $\mathcal{EL}$ TBoxes
   - Considering **complete knowledge** of attackers
4. Considering **Contextualized Description Logics**, e.g., ConDLs
   - Weakening ConDL axioms e.g.,
     $\texttt{Hospital} \sqsubseteq [\mathit{worksIn}.(\mathit{John}, \mathit{JosephStift})]$


References

1. **[DL2017]**:
   Franz Baader, Daniel Borchmann, and **Adrian Nuradiansyah**,
   Preliminary Results on the Identity Problem in Description Logic Ontologies,
   Montpellier, 2017.
2. **[JIST2017]**:
   Franz Baader, Daniel Borchmann, and **Adrian Nuradiansyah**,
   The Identity Problem in Description Logic Ontologies and Its Applications to View-Ba
   JIST 2017, Gold Coast, 2017.
3. **[KR2018]**:
   Franz Baader, Francesco Kriegel, **Adrian Nuradiansyah**, and Rafael Peñaloza,
   Making Repairs in Description Logics More Gentle, Tempe, 2018.
4. **JELIA2019**:
   Franz Baader, Francesco Kriegel, and **Adrian Nuradiansyah**,
   Privacy-Preserving Ontology Publishing for $\mathcal{EL}$ Instance Stores, Rende, 2019.
5. **KI2019**:
   Franz Baader and **Adrian Nuradiansyah**,
   Mixing Description Logics in Privacy-Preserving Ontology Publishing, Kassel,
   2019.

Thank You

RoSI